



HITACHI

LATAM Partner Summit FY26

Built to Grow. Powered by Data.



HITACHI

Brocade FC-SAN

The Compounding Threat:
Frontier AI and Quantum Decryption

Jesus Gonzalez Aceves

Brocade Senior SE – Mexico CACE

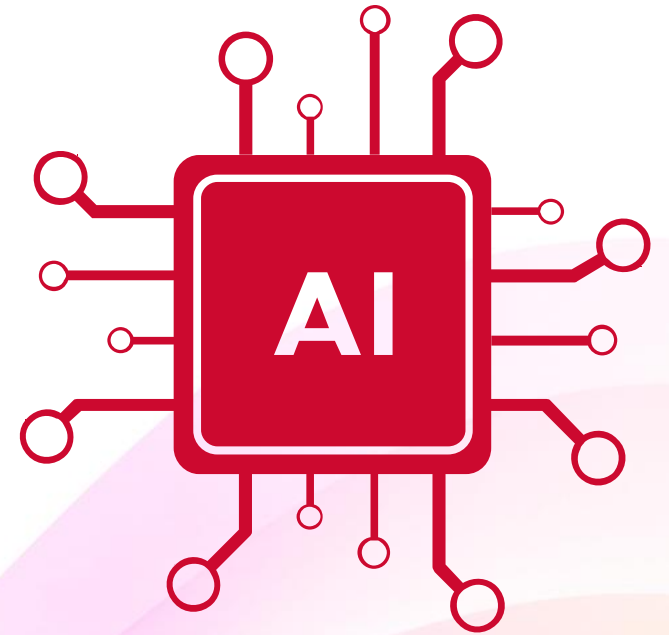
Broadcom

AI security era

Frontier agentic AI

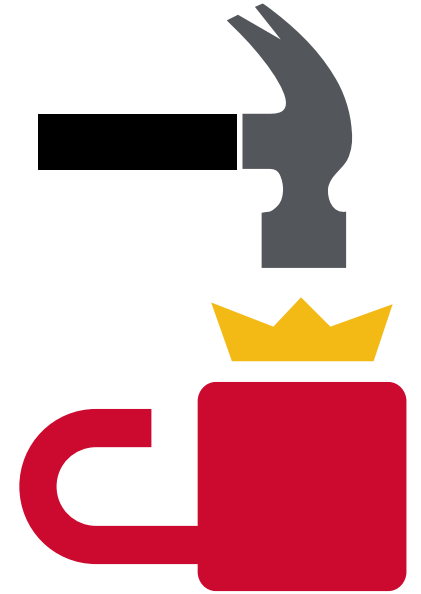
Frontier Agentic AI

- What is Frontier Agentic AI?
 - High-Reasoning Intelligence: The most advanced models capable of complex logic, strategy, and planning far beyond basic chatbots.
 - Autonomous Agency: Systems that transition from simply "answering questions" to independently "executing multi-step workflows."
 - Total Data Ingestion: The ability to instantly process and "understand" a company's entire codebase and proprietary data ecosystem.



Anthropic's Claude Mythos and Glasswing Overview

- What is Anthropic's Claude Mythos 5?
 - Autonomous Zero-Day Discovery: Finds and exploits critical, hidden vulnerabilities faster than teams of human researchers.
 - A "Double-Edged" Capability: Possesses equal capability to write malicious exploit code or engineer a defensive patch.
- What is Project Glasswing?
 - Anthropic's internal, highly restricted sandbox, available only to vetted enterprise partners and governments designed to contain and stress-test the unrestricted capabilities of Claude Mythos 5.
- How has Broadcom been involved in Project Glasswing?
 - Broadcom was an initial partner granted early access to Claude Mythos 5.
 - Leveraged the model's autonomous reasoning to scan, find, and patch hidden vulnerabilities across the portfolio.
 - Results of testing with Glasswing and Claude Mythos 5 are under NDA.



Frontier AI: The Threat is Real. The Threat is Now

- Legacy Gen 5 and Gen 6 hardware and software are vulnerable due to architectural and resource constraints.
- Frontier AI eliminates barriers to entry and enables anyone to exploit vulnerabilities.
- Because agents are constantly learning, they are multiplying and accelerating attack vectors at an unprecedented scale.
- Countering agentic AI demands an expert threat response team that leverages frontier AI to autonomously scan, identify, and remediate vulnerabilities.



Brocade's PSIRT Process Updated with AI Scanning

Continuous Robust Security Vulnerability Intake



SAST and DAST Security Scanning

Continuous scanning with multiple scanning tools: Black Duck, Qualys, Nessus, Coverity, and Burp Suite tools

Exploit Monitoring

Continuous tracking of databases, security research, FIRST, Mitre, and vulnerability intelligence sources.



AI Model Security Scanning

Moving from passive signature detection to active threat prediction: Context aware prioritization

Customer & OEM Input

Issues identified and raised directly with engineering or through official support channels.



Penetration Testing

Regular assessment through internally driven threat assessment security testing and specialized external 3rd party testing.

Direct Reporting

Researchers reporting directly to the Product Security Team: brocade.sirt@Broadcom.com



Frontier AI Scanning Vulnerability Response

Comprehensive Scanning of all BSN products

- **Zero** Critical Severity findings
- **100% completed** scanning all latest software product versions
- **Risk Assessment** evaluation conducted on all identified vulnerabilities

Continued Scanning:

Future scans and security updates will be focused on latest software versions

High Risk

Address immediately in latest releases

Crafted attacks through memory corruption or privilege escalation, leading to full system compromise

FOS 10.0.1 SANnav 3.0.1a ASCG 3.5.0
Brocade PSIRT process maintained for legacy support

Medium and Lower Risk

Address in next major releases

Vulnerabilities exposed by lateral movement via exploited network endpoints, and zero trust network hardening

FOS 10.1.0 SANnav 3.1.0 ASCG 3.6.0

Take Action to Prevent Crafted Attacks

Immediate Action

Migrate to Gen 8 ASAP

Address Hardware Limitations

Legacy Gen 5 and 6 hardware/software are vulnerable due to architectural and resource constraints

Recommendation

Migrate to Gen 8 hardware to ensure access to Frontier AI security updates and PQC compliance

Gen 5 is critically exposed today and Gen 6 cannot remain protected

FOS 10.0.1 and later versions only run on Gen 7 and Gen 8 hardware.

Ongoing Protection

Upgrade to Target Path

Upgrade Fabric OS

Upgrade to a hardened version of Fabric OS to prevent active threats

Recommendation

FOS v10.0.1 now for Gen 8 and Gen 7 switches already running FOS 10.x
FOS v10.0.1a later this year for Gen 7
FOS v9.2.2d for Gen 6 (GA 8/25/26)

SANnav v3.0.1a (GA 8/12/26)
ASCG 3.5.0 (GA 8/14/26)

Strategic Planning

Stay on Target Path

Deploy Latest Updates

Upgrade to newer Target Path versions as they are released to maintain defense

Recommendation

Latest FOS v10.0.1x Target Path versions
Latest SANnav and ASCG patches

Then when available to fully harden against lateral movement exploits
FOS v10.1.0x Target Path
SANnav v3.1.0x Target Path
ASCG v3.6.0

All content and schedules subject to change

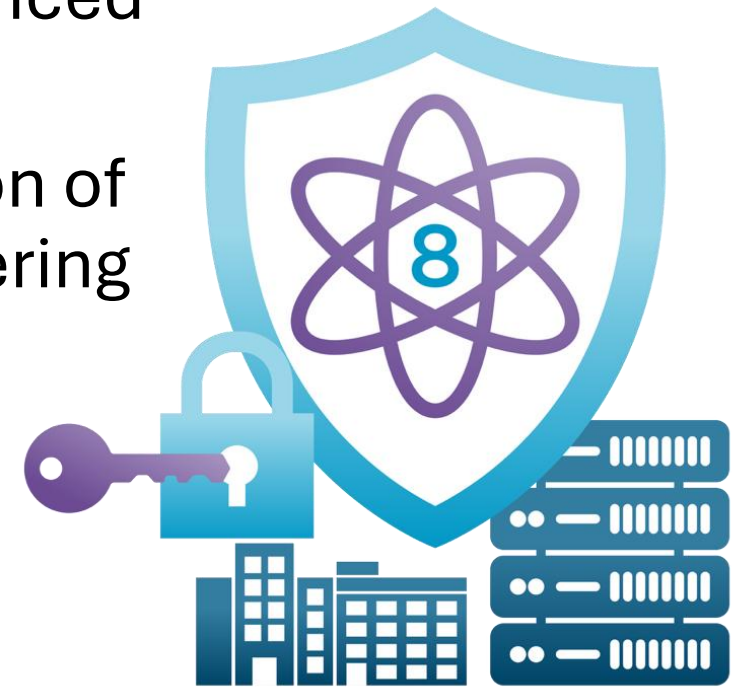
Quantum Safe

Post Quantum
Decryption Security

Enabling a Quantum-Safe SAN for the Enterprise AI Era

Protect from quantum computing and cybersecurity threats

- Protect SAN fabrics against attacks with advanced cryptographic algorithms
- Reduce the risk of hijacking and the installation of malicious software with enhanced anti-tampering technology
- Minimize attack surface with embedded mandatory access controls
- Monitor and alert for security configuration changes and events
- Validate the integrity and security of Brocade hardware and software



Brocade®
GEN8
FIBRE CHANNEL

Is Your Storage Network Quantum Safe?

Time to Move to New Post Quantum Cryptography (PQC)

Brocade Gen 8 is quantum-safe, protecting sensitive data and critical infrastructure from future quantum computers

- Brocade fabrics secures data flows in-flight within and across data centers with quantum-resistant, AES 256-bit encryption
- Brocade Gen 8 supports Post Quantum Cryptography in FOS v10.x
 - SSH and SSH KEX
 - TLS Sign/Verify and Key Encapsulation
 - Stronger ciphers for symmetric encryption and hashes
 - IKEv2 with PQC for Extension

Post-Quantum Cryptographic Algorithms



Public-key

ML-DSA (CRYSTALS-Dilithium)
ML-KEM (CRYSTALS-Kyber)

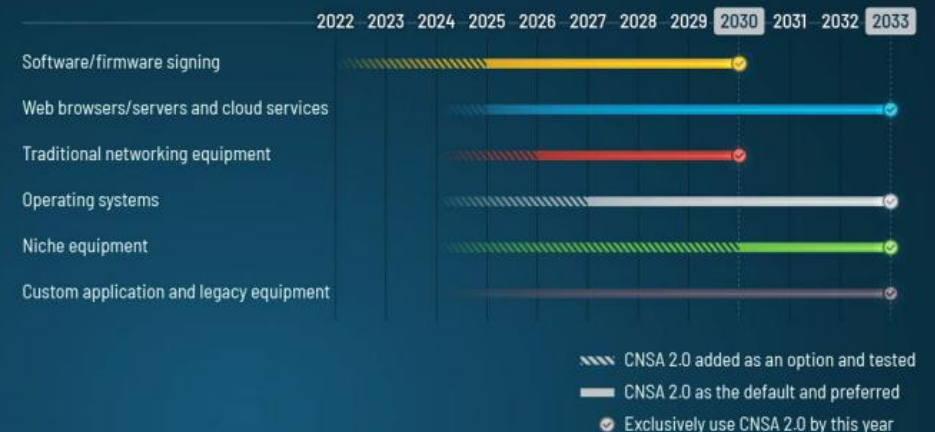
Symmetric-key

Advanced Encryption Standard (AES)
Secure Hash Algorithm (SHA)

Software and Firmware Updates

Xtended Merkle Signature Scheme (XMSS)
Leighton-Micali Signature (LMS)

CNSA 2.0 Timeline



Brocade Gen 8

Secure Your Data Assets on the Most
Secure Network in the Data Center

Clocks Ticking !!!

Three clocks are running at once – and they don't run on the same schedule as a typical refresh cycle.



Harvest Now, Decrypt Later

Adversaries are capturing encrypted traffic today, banking on quantum decryption capability arriving before this hardware is retired.



2030 PQC Compliance Deadline

Regulatory timelines under **EO 14409** and **EO 14413** push agencies and critical infrastructure toward post-quantum migration on a fixed clock, not a flexible one.



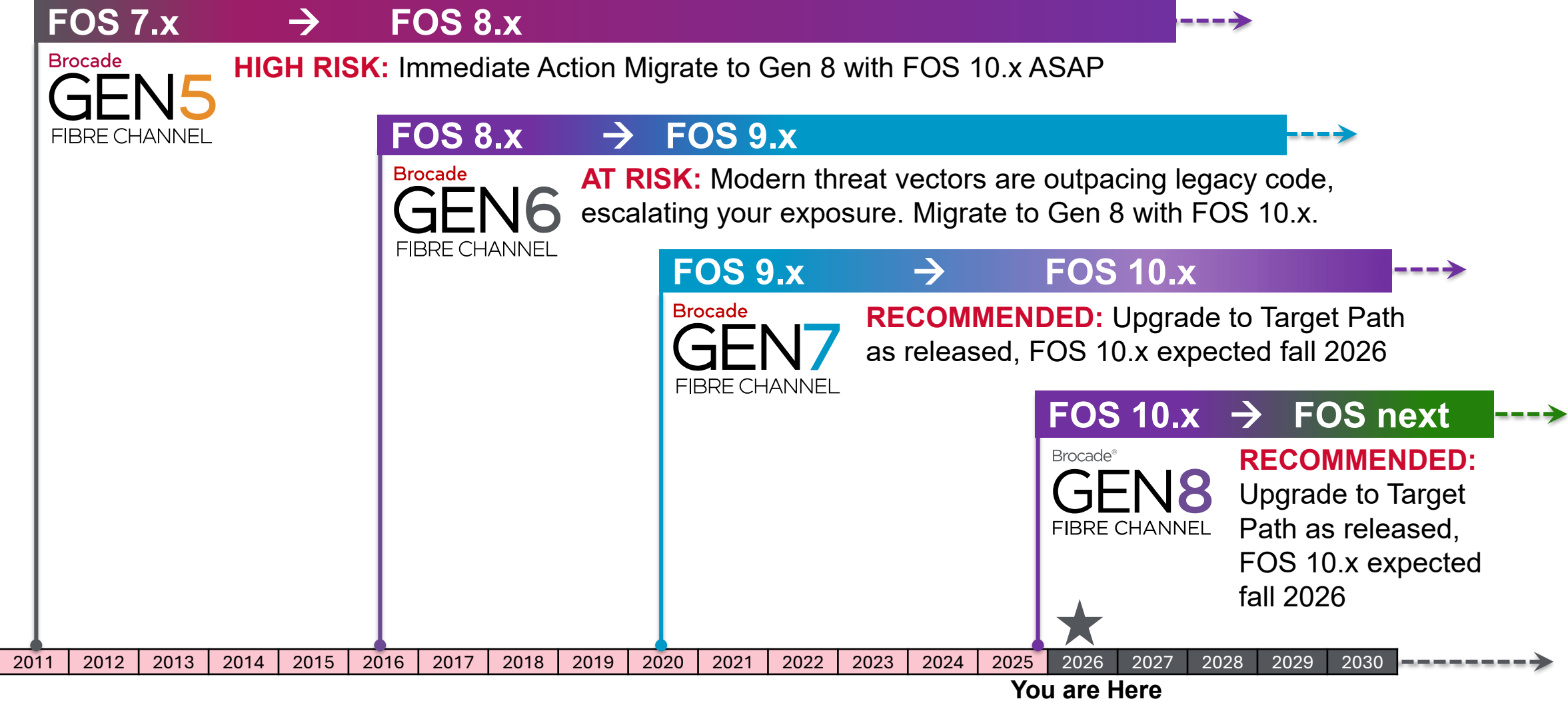
AI-Accelerated Attackers

The same frontier AI capability improving defensive software is available to attackers scanning for exposure — the advantage goes to whoever moves first.

Every quarter without a modernization plan is a quarter competitors — and adversaries — use to close the gap.

Run Latest Fabric OS and Software to Prevent AI Attacks

Gen 5 and Gen 6 are at risk! FOS 10.x only runs on Gen 7 and Gen 8 hardware



Time to Refresh: Products Without Frontier AI Security Updates

What does FOS End-of-Availability (EOA) mean?

➡ No Planned Security Updates

Still supported, but no planned software updates, fixes, or AI security scans

What does End-of-Support (EOS) mean?

➡ Zero Security Updates

No software updates, fixes or future AI scans

➡ Restricted Support

Multi-device fabric troubleshooting blocked until EOS gear is removed

➡ SANnav Monitoring Ends

Brocade SANnav will no longer monitor assets post-EOS

Gen 5 and Gen 6 Hardware: Frontier AI Threat is High
Upgrade to Brocade Gen 8 and FOS 10.x for AI-hardened storage networking

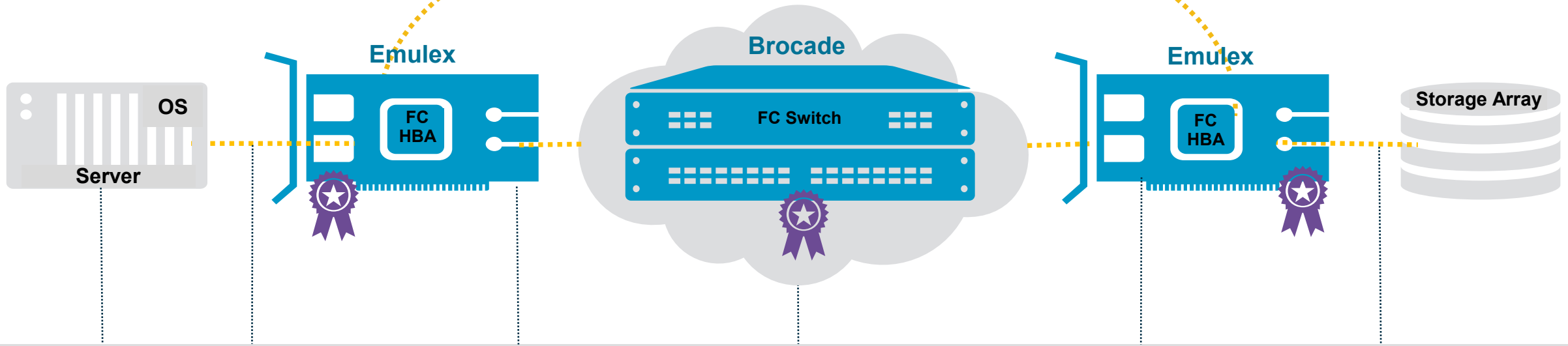
Generationz	Products	Frontier AI Threat Status	Max FOS Level	Fabric OS End-of-Availability	End-of-Support	Suggested Replacements
Gen 6 Directors	Brocade X6-8 Brocade X6-4	At Risk!	9.x	July 15, 2026	July 15, 2029	Brocade X8-8 Brocade X8-4
Gen 6 Switch	Brocade G620	At Risk!	9.x	Jan 31, 2027	Jan 31, 2030	Brocade G820
Gen 5 Directors	Brocade 8510-8 Brocade 8510-4	At Risk!	8.x	April 30, 2023	April 30, 2025	Brocade X8-8 Brocade X8-4
Gen 5 Switch	Brocade 6520	High Risk!	8.x	Sept 21, 2024	Sept 21, 2027	Brocade G730
Gen 5 Switch	Brocade 6510	High Risk!	8.x	June 17, 2023	June 17, 2025	Brocade G820
Gen 5 Switch	Brocade 6505	High Risk!	8.x	April 30, 2023	August 31, 2025	Brocade G710
Gen 5 Extension	Brocade 7840	High Risk!	8.x	Feb 28, 2026	Feb28, 2029	Brocade 7850

Protect Your Data with Quantum-Safe In-flight Encryption

Plug-and-Play in-flight encryption everywhere at full performance



End-to-End In-flight Encryption



Signed Drivers



CPU - HBA
Attestation
(SPDM)



Silicon Root
of Trust



Silicon Root
of Trust

Federated
Authentication
(FA)



Silicon Root
of Trust



CPU - HBA
Authentication
(SPDM)

Zero
Trust

Brocade Gen 8: AI Threat-Secure and Quantum Safe

The most secure, high-performance storage network in the data center

- AI threat-secure FOS v10.x, SANnav v3.x, and ASC Gateway v3.x software
 - Proactive frontier AI scanning and defensive patching of learned threats minimize vulnerabilities.
 - Focused and active threat response engineering accelerates fixes.
 - Enforced access control minimizes attack surface.
- Quantum-safe Gen 8 hardware
 - Post-quantum cryptography protects against future quantum compute attacks.
 - Enhanced anti-tampering technology eliminates installation of malicious code.

Brocade®

GEN8
FIBRE CHANNEL



Brocade Education

Free 24/7 training and knowledge assessment exams

Over 80 free online training courses grouped into topical playlists

- Fibre Channel SAN basics
- Gen 6 & 7 switches and directors
- Protocol training (FC / NVMe / FICON)
- Installation and configuration
- SANnav
- Advanced features



✓ Recognition ✓ Printable certificate ✓ Permanent transcript

Free knowledge assessment exams

- Gain new knowledge and recognition
- Downloadable certificate
- Permanent transcript on learning portal
- The same high-quality test questions found in industry certification exams without the requirement of a proctored environment

Quarterly webcasts

- Direct-to-end user interactive live webcasts

Brocade sales team for HV – Americas and LATAM



Sales team Americas

Michael Fahey
HV OEM Alliance Manager
Michael.Fahey@broadcom.com
HV Central US, LATAM & Canada

Chris Sorensen
Emulex Alliance Director
Chris.Sorensen@broadcom.com

Ray Leonard
DCSG Marketing Ethernet
Ray.Leonard@broadcom.com



Brocade Sales team LATAM

Samuel Xavier
Sr. Director LATAM
samuel.xavier@broadcom.com
Brasil

Jose D'Antonio
Regional Sales Mgr
Mexico CACE SSA
jose.dantonio@broadcom.com
Argentina

Antonio Carlos Lopes
Territory Account Manager
antonio.lopes@broadcom.com
Brasil

Jean Linakis
Territory Account Manager
jean.linakis@broadcom.com
Brasil

Iván Calderón Carroza
FAE SSA
ivan.calderon@broadcom.com
Chile

Jesus Gonzalez Aceves
FAE Mexico CACE
jesus.gonzalez-aceves@broadcom.com
Mexico

Marcio Matiello
FAE
marcio.matiello@broadcom.com
Brasil



Gracias

Jesus Gonzalez Aceves

Brocade Senior SE – Mexico CACE

Broadcom